Principles of Secure Software Design

Margus Freudenthal

What is scope of the system?

What is scope of the system?

- A component, such as smartcard or a PC

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure
- Above + applications

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure
- Above + applications
- Above + IT staff

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure
- Above + applications
- Above + IT staff
- Above + internal users and management

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure
- Above + applications
- Above + IT staff
- Above + internal users and management
- Above + customers and external users

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure
- Above + applications
- Above + IT staff
- Above + internal users and management
- Above + customers and external users
- Above + environment

What is scope of the system?

- A component, such as smartcard or a PC
- Above + operating system, network and other infrastructure
- Above + applications
- Above + IT staff
- Above + internal users and management
- Above + customers and external users
- Above + environment

Everything

What it's about?

- Security issues in high-level system design
- Protecting against the right threats
- Having the right amount of security measures
- The focus is on system, not software

Who am I?

- Name: Margus Freudenthal
- MSc at TTU („Personal Security Environments”), PhD student at TU
- Worked on:
  - Digital notary service
  - Time-stamping service
  - X-Road security infrastructure
  - Estonian Digital signature standards

Main books

- „Security Engineering” by Ross Anderson
- „Secrets and Lies” by Bruce Schneier
- Other readings suggested in lectures

Also in cinemas...

- MTAT.03.247 „Principles of Secure Software Design: Project Work”
- Security analysis of a reasonably complex system
- Teams of 2 or 3
- Results in report and presentation

Examples of systems

- Electronic bus tickets
- Internet voting
- Offline cash
- Some Internet environment
  - Orkut
  - Facebook
  - Rate.ee
- Some innovative mobile service

Contents of the report

- Description of the system
  - Purpose
  - Parties
  - Assets
- Security policy
  - What are the rules
  - What are the risks
- What will we defend against?
- How?

Contents of the report (2)

- Some cost estimations
  - Cost of attack
  - Cost of defence
- Conclusion
  - What should be done
  - Most important security measures
  - Is the whole project reasonable?

Lectures

- Initial lecture – terminology, concepts, some philosophy
- Security and usability
- Multilevel security and various data protection issues
- Monitoring systems
- Eavesdropping (physical and logical)

Lectures (2)

- Content protection
- Banking and bookkeeping
- On-line games
- Case study: X-Road
- Case study: digital signatures (in legal context)
- Developing cryptographic protocols
- Strategies for developing secure software

On with the lecture...

Some terminology

- TODO: picture

Some terminology (2)

- Trusted system – a component or system whose failure will break the security policy
  - Trustworthy – component or system that will not fail

Some terminology (3)

- Security policy – succinct statements of system's protection strategy
  - e.g. „each credit must be matched by an equal and opposite debit, and all transactions over $1000 must be authorized by two managers”
- Security target – more detailed specification which describes how the security policy is implemented

Example of security issue

- Suppose the Unix ls command contains buffer overflow when processing input parameters
- Is this a vulnerability?

Example of security issue (2)

- For ordinary command-line use, this is reliability issue
- It becomes vulnerability when ls is used in a boundary between two security zones
  - For example, ftp server that separates untrusted Internet from trusted file system

Freudenthal's creed

- Security issues arise at the boundary between zones with different security policies
- Therefore, defect in program is not necessarily a security flaw, unless this defect propagates to the perimeter

Role of security measures

- Organization's goal is usually not to secure stuff
- Instead:
  - Make profit selling books
  - Provide better public service to citizens
- Sometimes, less security can better fulfill organization's goals

Example of security trade-off

- Supermarkets have considerably higher risk of theft than smaller, over the counter stores
- However...
  - Economy of scale
  - Less personnel
- It gets better
  - Self-service checkout
  - Customers can weigh items themselves

Manage risks

- The important point is not to prevent bad things
  - Usually, preventing is impossible
- The important point is to have reasonable amount of leftover risk
  - E.g. supermarket has leftover risk of thefts $10000/year
- There is no point on spending more than leftover risk on security measures

Important

- When doing risk assessment, look at risks of people
- For manager, it's risk of not earning profit
- For employee, it's not getting work done
- When analyzing a system, look at people's motives
- Security problems rise from conflicts of interest

That's it